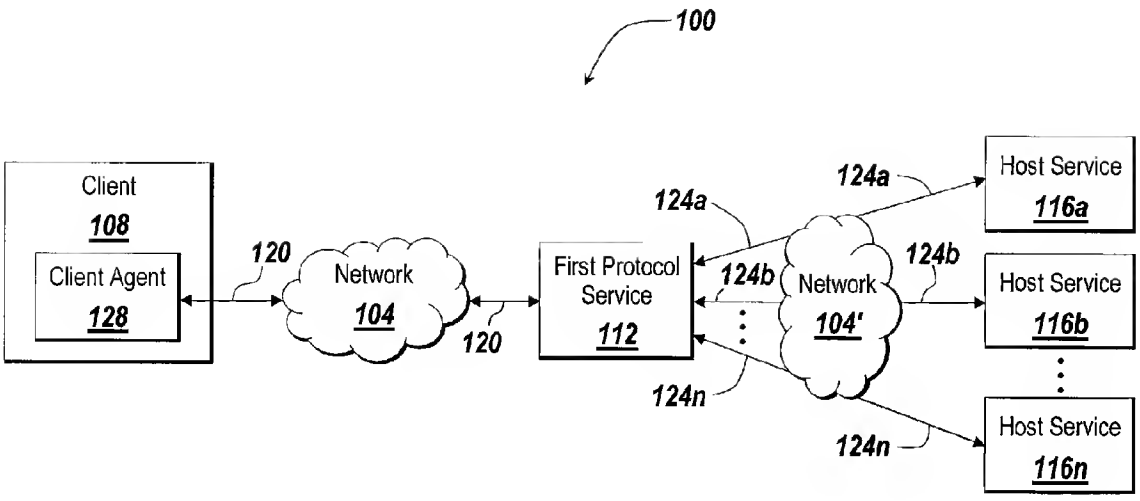
100
Client
108
Client Agent
128
120
Network
104
120
First Protocol Service
112
124a
124b
124n
Network
104'
124a
124b
124n
Host Service
116a
Host Service
116b
Host Service
116n

Fig. 1A

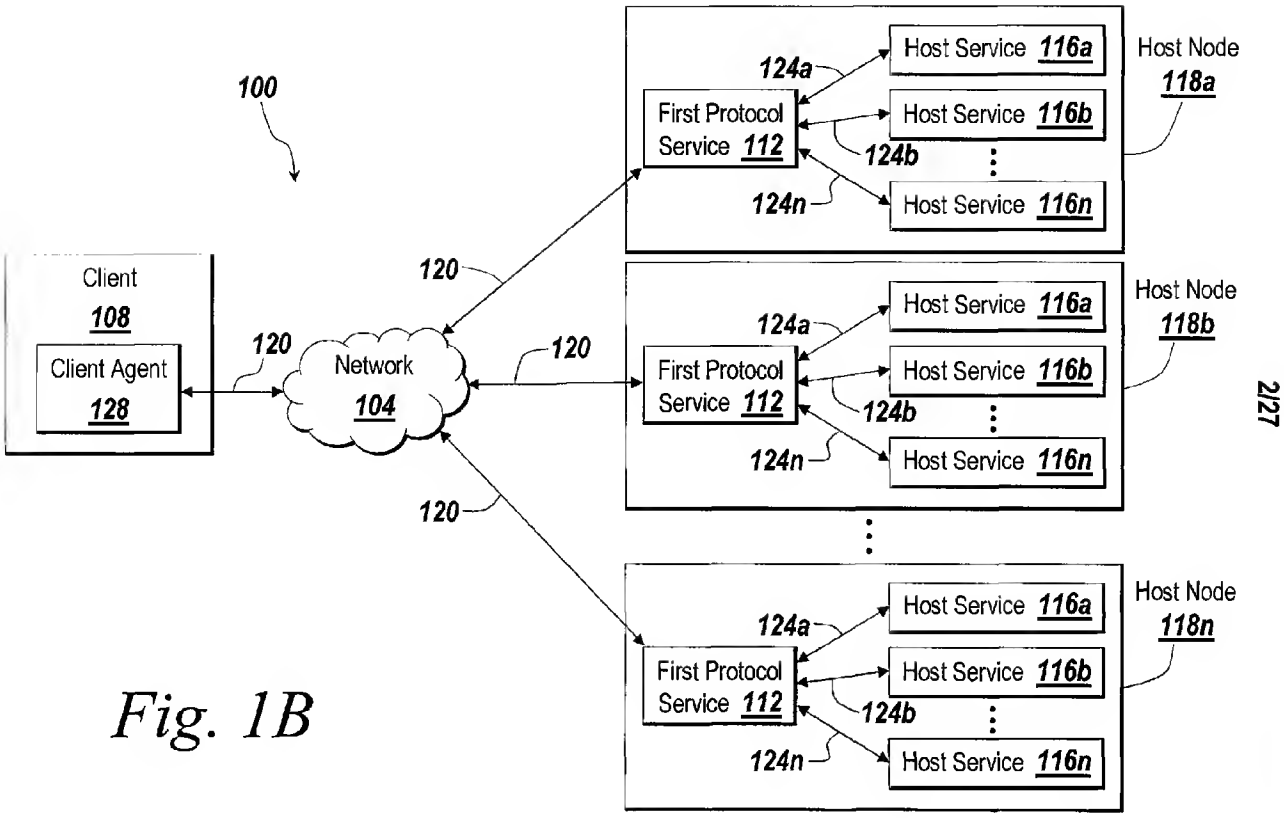
100
Client
108
Client Agent
128
120
Network
104
120
120
120
First Protocol Service 112
124a
124b
124n
Host Service 116a
Host Service 116b
Host Service 116n
Host Node 118a
Host Node 118b
Host Node 118n

Fig. 1B

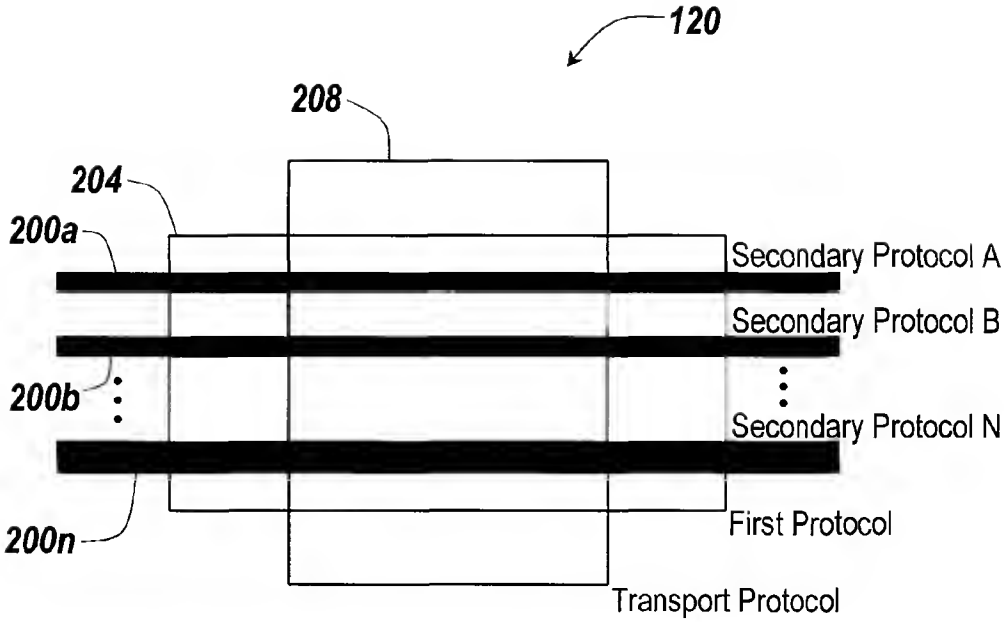
120
208
204
200a
Secondary Protocol A
Secondary Protocol B
200b
Secondary Protocol N
200n
First Protocol
Transport Protocol

Fig. 2A

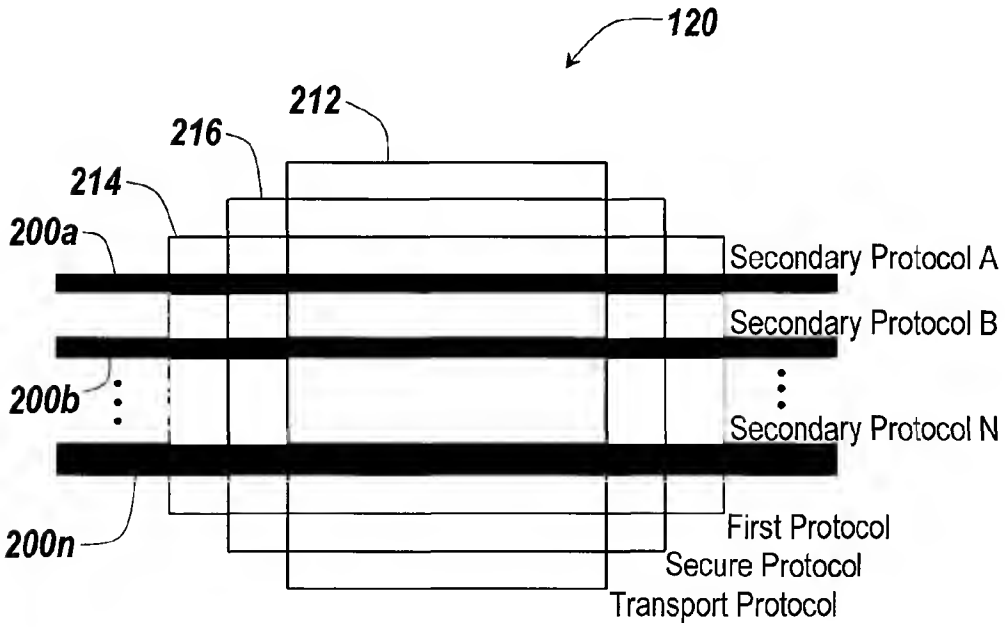
120
212
216
214
200a
Secondary Protocol A
Secondary Protocol B
200b
Secondary Protocol N
200n
First Protocol
Secure Protocol
Transport Protocol

Fig. 2B

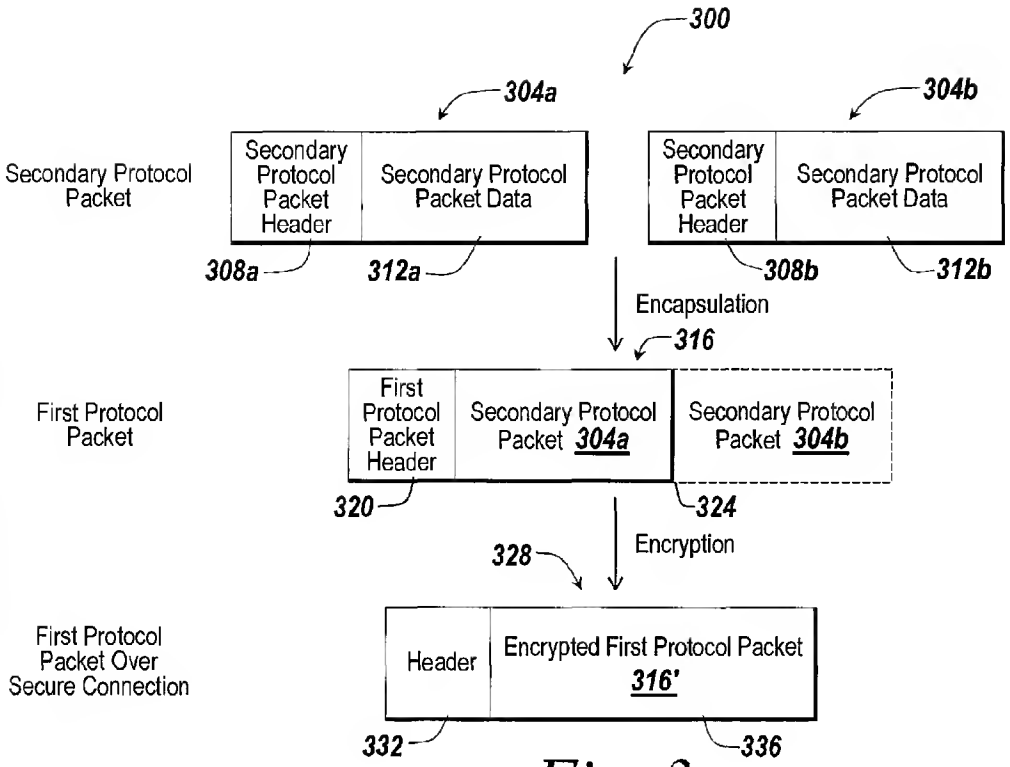
300
304a
304b
Secondary Protocol Packet
Secondary Protocol Packet Header
Secondary Protocol Packet Data
Secondary Protocol Packet Header
Secondary Protocol Packet Data
308a
312a
308b
312b
Encapsulation
316
First Protocol Packet
First Protocol Packet Header
Secondary Protocol Packet 304a
Secondary Protocol Packet 304b
320
324
328
Encryption
First Protocol Packet Over Secure Connection
Header
Encrypted First Protocol Packet 316'
332
336

Fig. 3

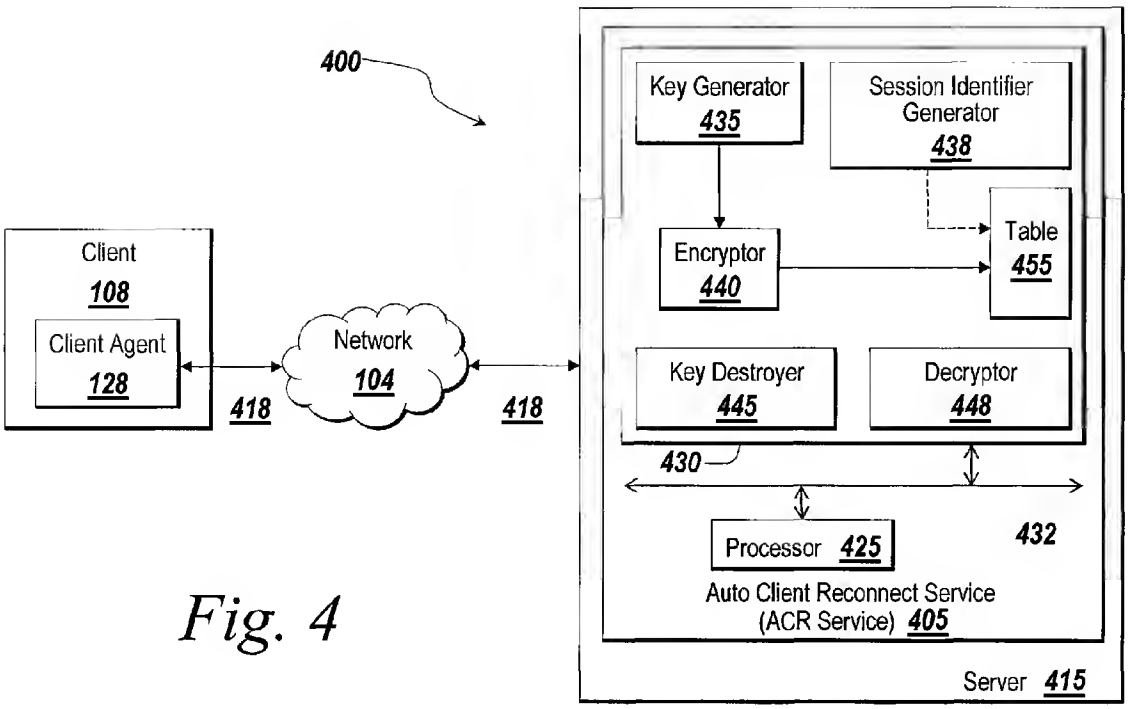
400
Client
108
Client Agent
128
418
Network
104
418
Key Generator
435
Session Identifier Generator
438
Table
455
Encryptor
440
Key Destroyer
445
Decryptor
448
430
Processor 425
432
Auto Client Reconnect Service (ACR Service) 405
Server 415

Fig. 4

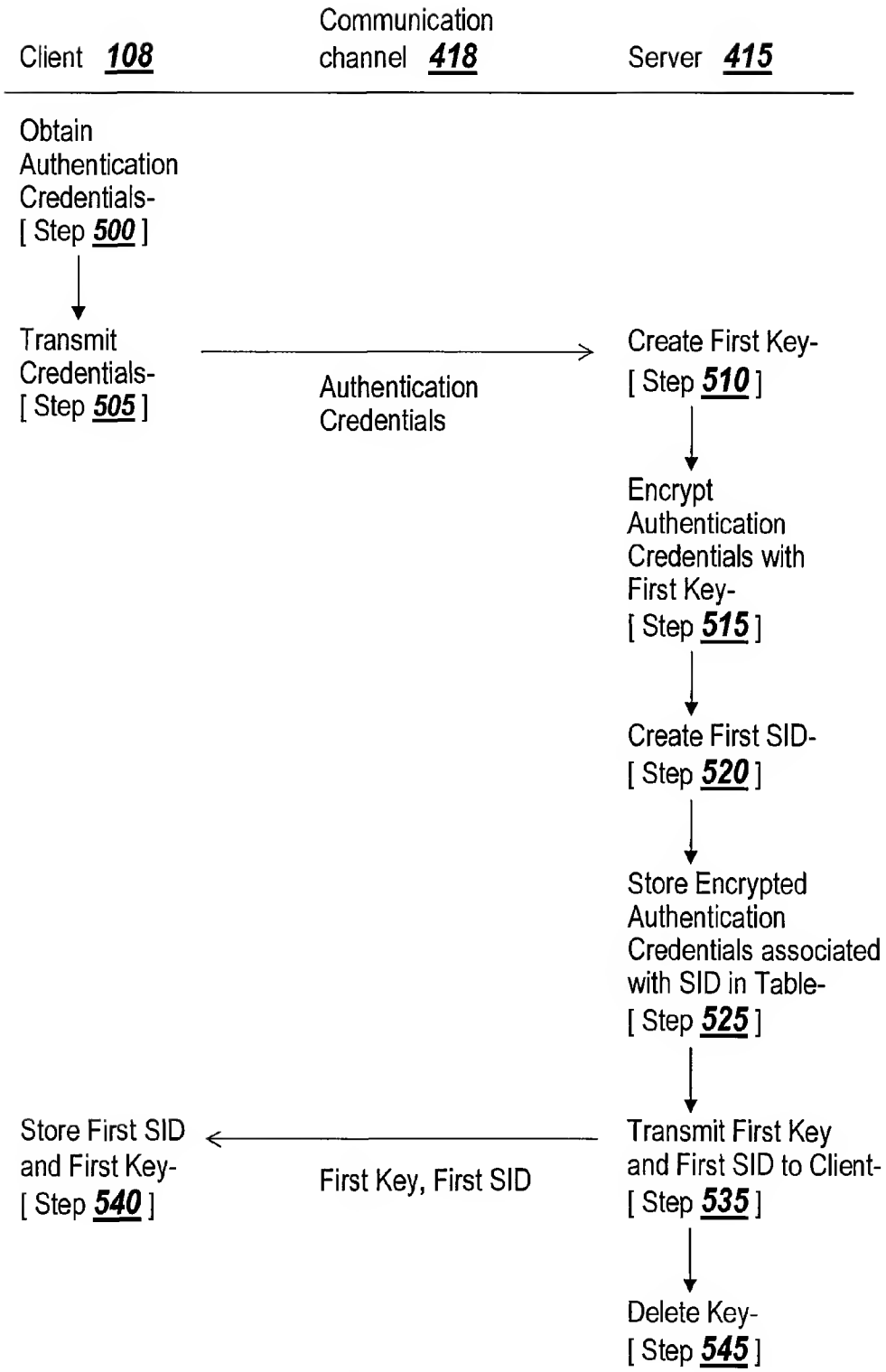
Client 108
Communication channel 418
Server 415
Obtain Authentication Credentials- [Step 500]
Transmit Credentials- [Step 505]
Authentication Credentials
Create First Key- [Step 510]
Encrypt Authentication Credentials with First Key- [Step 515]
Create First SID- [Step 520]
Store Encrypted Authentication Credentials associated with SID in Table- [Step 525]
Transmit First Key and First SID to Client- [Step 535]
First Key, First SID
Store First SID and First Key- [Step 540]
Delete Key- [Step 545]

Fig. 5A

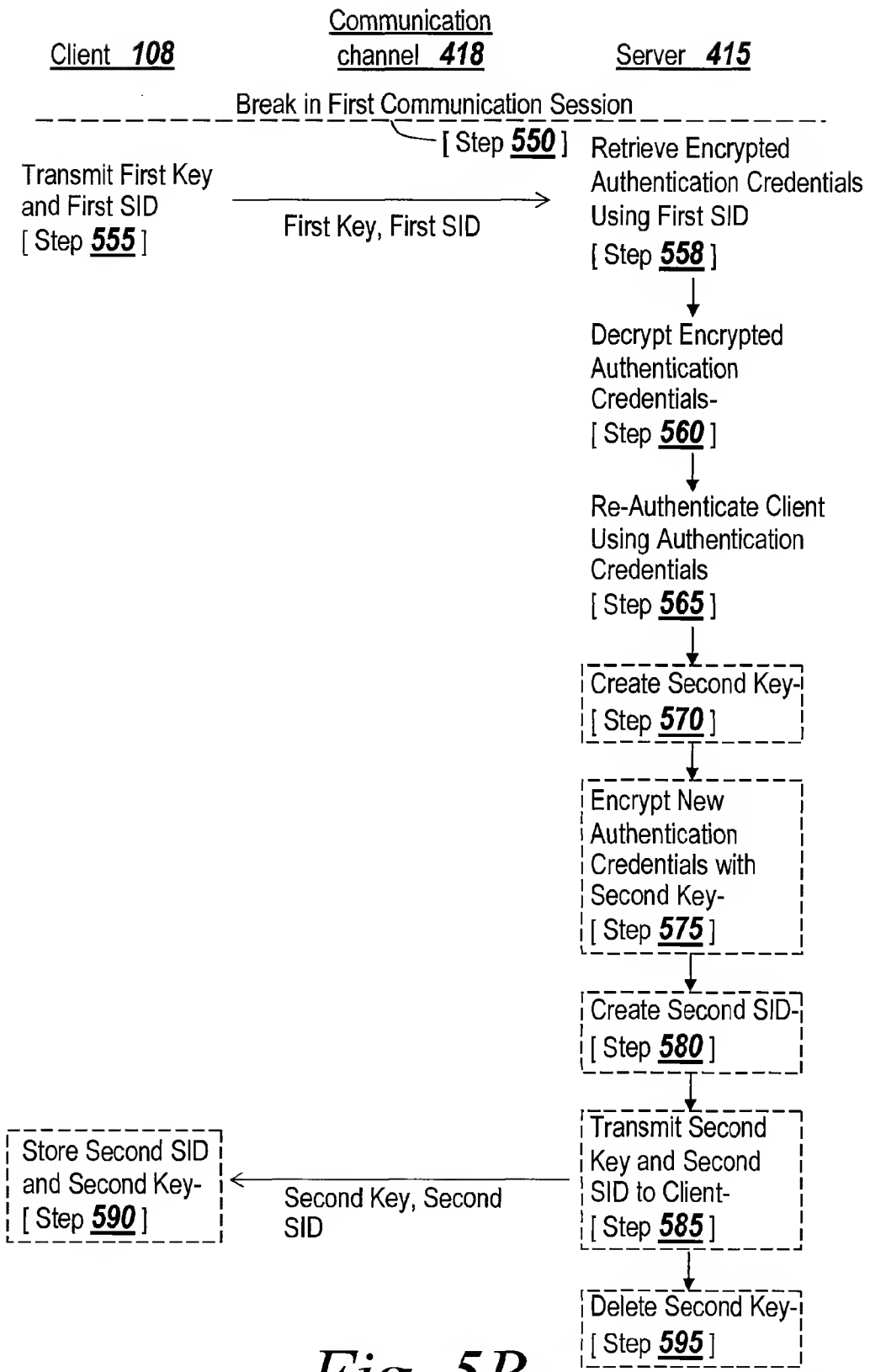
Client 108
Communication channel 418
Server 415
Break in First Communication Session
[Step 550]
Transmit First Key and First SID [Step 555]
First Key, First SID
Retrieve Encrypted Authentication Credentials Using First SID [Step 558]
Decrypt Encrypted Authentication Credentials- [Step 560]
Re-Authenticate Client Using Authentication Credentials [Step 565]
Create Second Key- [Step 570]
Encrypt New Authentication Credentials with Second Key- [Step 575]
Create Second SID- [Step 580]
Transmit Second Key and Second SID to Client- [Step 585]
Second Key, Second SID
Store Second SID and Second Key- [Step 590]
Delete Second Key- [Step 595]

Fig. 5B

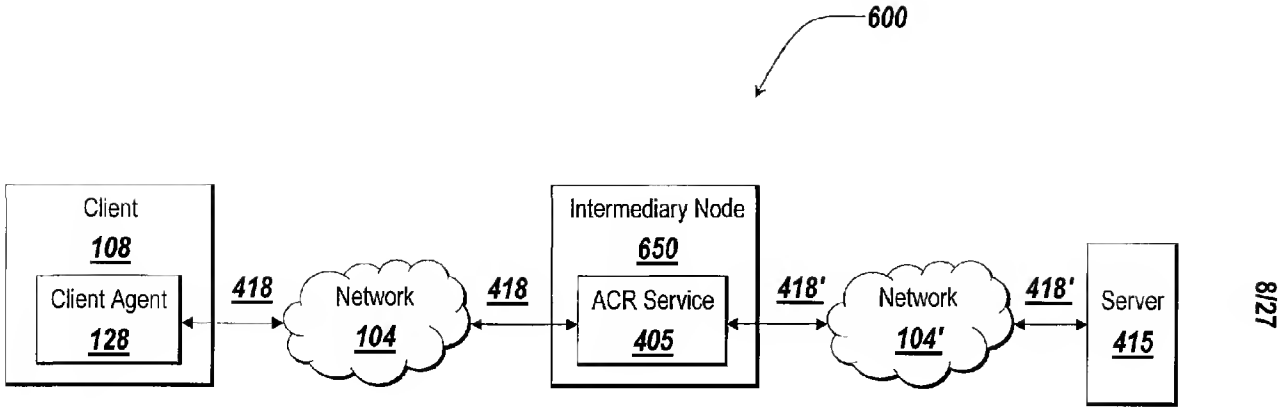
600
Client
108
Client Agent
128
418
Network
104
418
Intermediary Node
650
ACR Service
405
418'
Network
104'
418'
Server
415
8127

Fig. 6

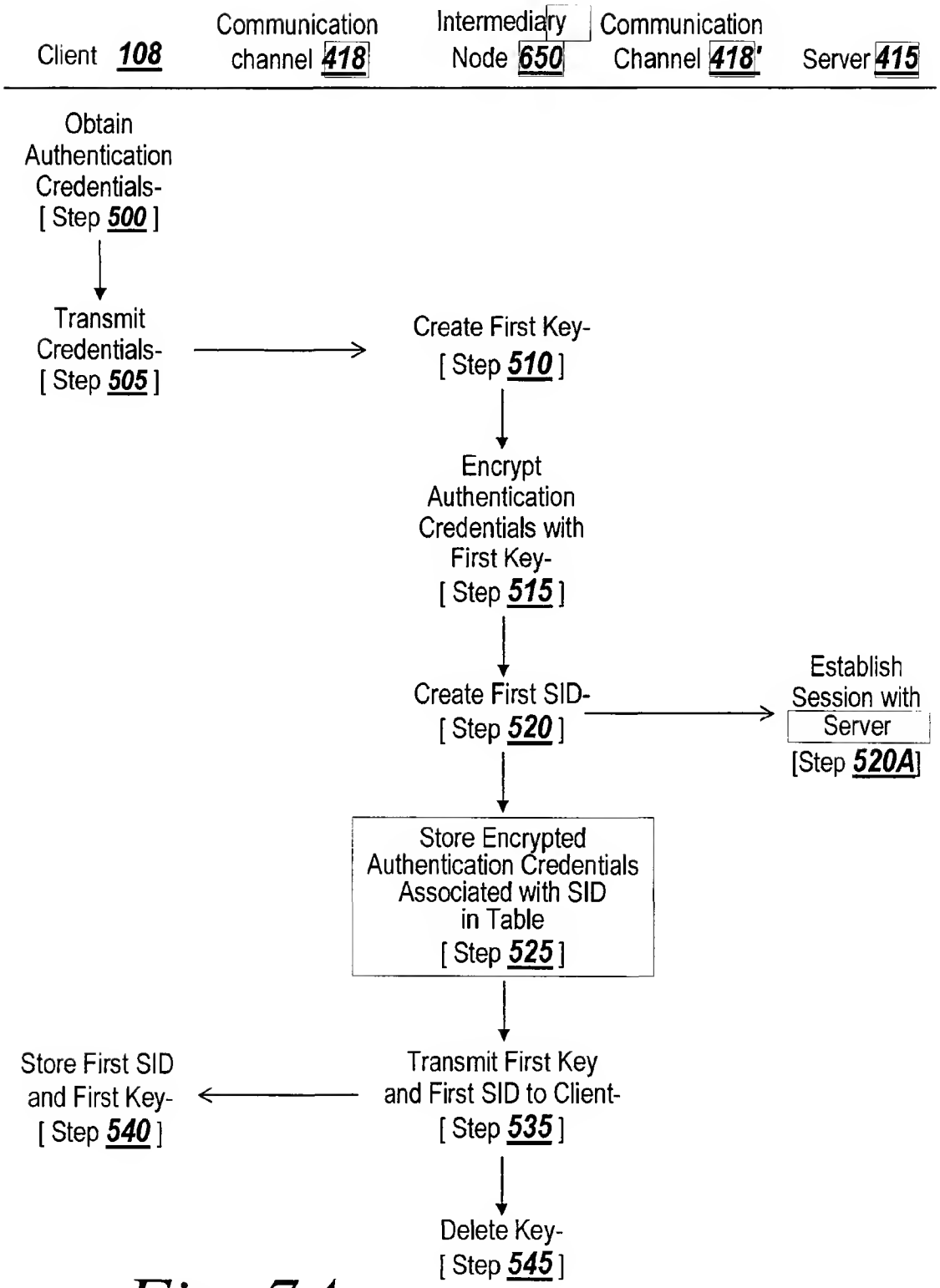
Client 108
Communication channel 418
Intermediary Node 650
Communication Channel 418'
Server 415
Obtain Authentication Credentials- [Step 500]
Transmit Credentials- [Step 505]
Create First Key- [Step 510]
Encrypt Authentication Credentials with First Key- [Step 515]
Create First SID- [Step 520]
Establish Session with Server [Step 520A]
Store Encrypted Authentication Credentials Associated with SID in Table [Step 525]
Transmit First Key and First SID to Client- [Step 535]
Store First SID and First Key- [Step 540]
Delete Key- [Step 545]

Fig. 7A

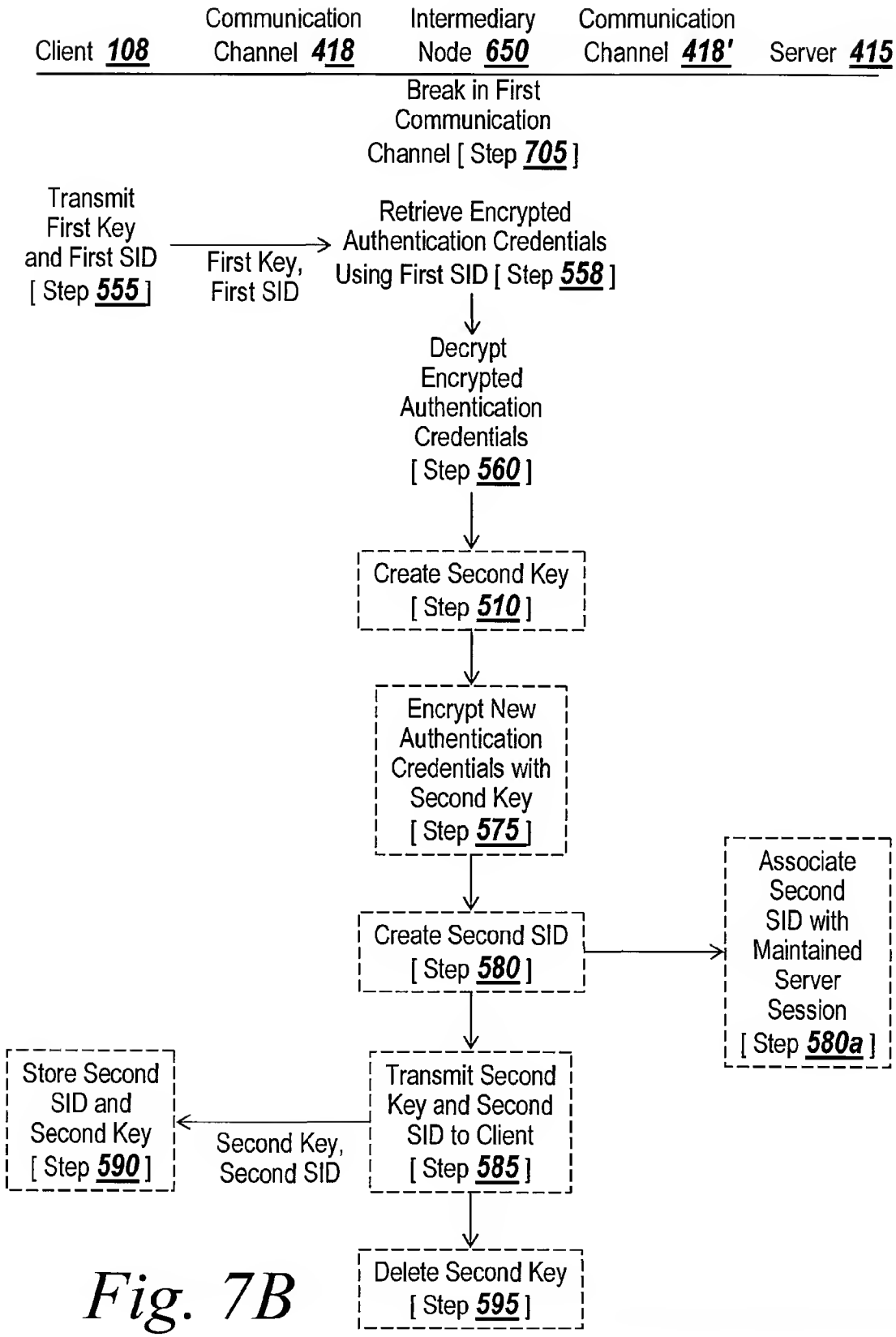
Client 108
Communication Channel 418
Intermediary Node 650
Communication Channel 418'
Server 415
Break in First Communication Channel [Step 705]
Transmit First Key and First SID [Step 555]
First Key, First SID
Retrieve Encrypted Authentication Credentials Using First SID [Step 558]
Decrypt Encrypted Authentication Credentials [Step 560]
Create Second Key [Step 510]
Encrypt New Authentication Credentials with Second Key [Step 575]
Create Second SID [Step 580]
Associate Second SID with Maintained Server Session [Step 580a]
Transmit Second Key and Second SID to Client [Step 585]
Second Key, Second SID
Store Second SID and Second Key [Step 590]
Delete Second Key [Step 595]

Fig. 7B

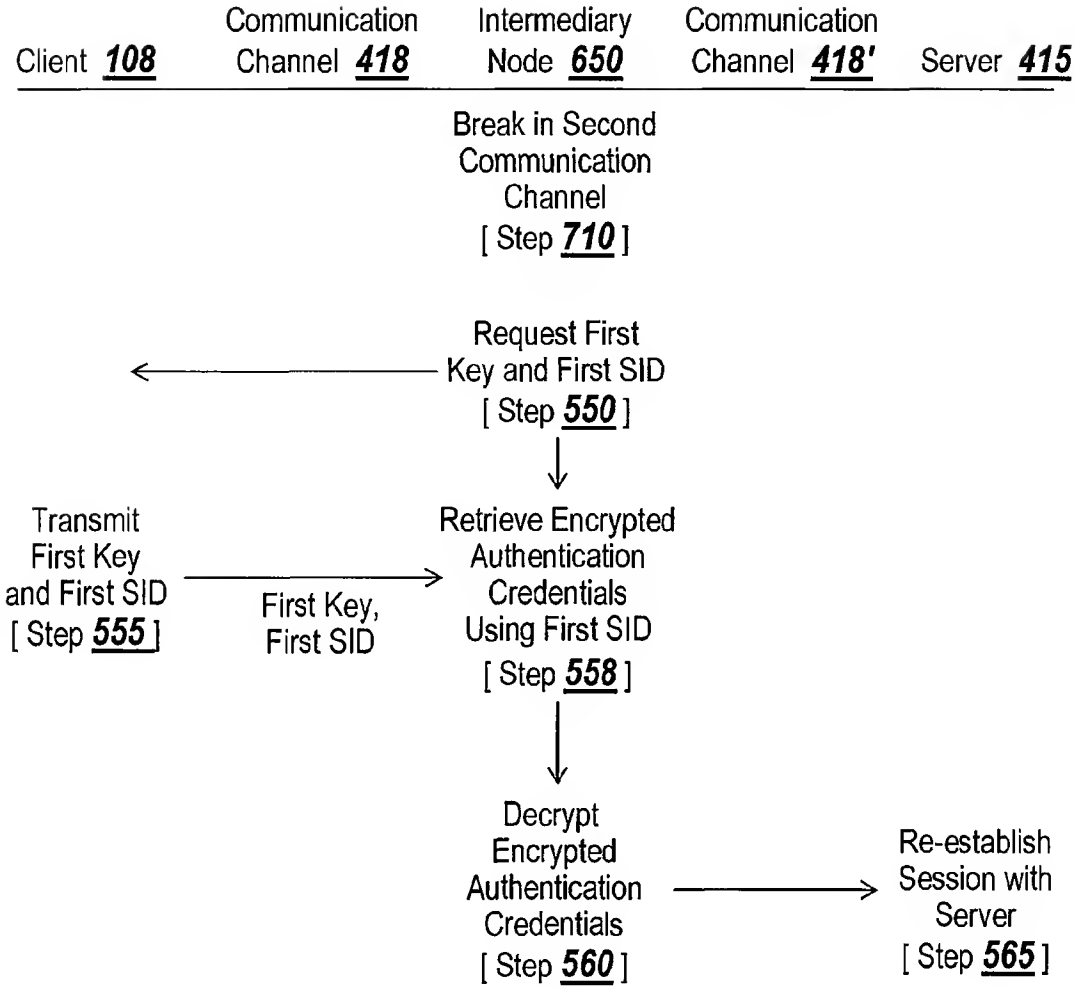
Client 108
Communication Channel 418
Intermediary Node 650
Communication Channel 418'
Server 415
Break in Second Communication Channel [Step 710]
Request First Key and First SID [Step 550]
Transmit First Key and First SID [Step 555]
First Key, First SID
Retrieve Encrypted Authentication Credentials Using First SID [Step 558]
Decrypt Encrypted Authentication Credentials [Step 560]
Re-establish Session with Server [Step 565]

Fig. 7C

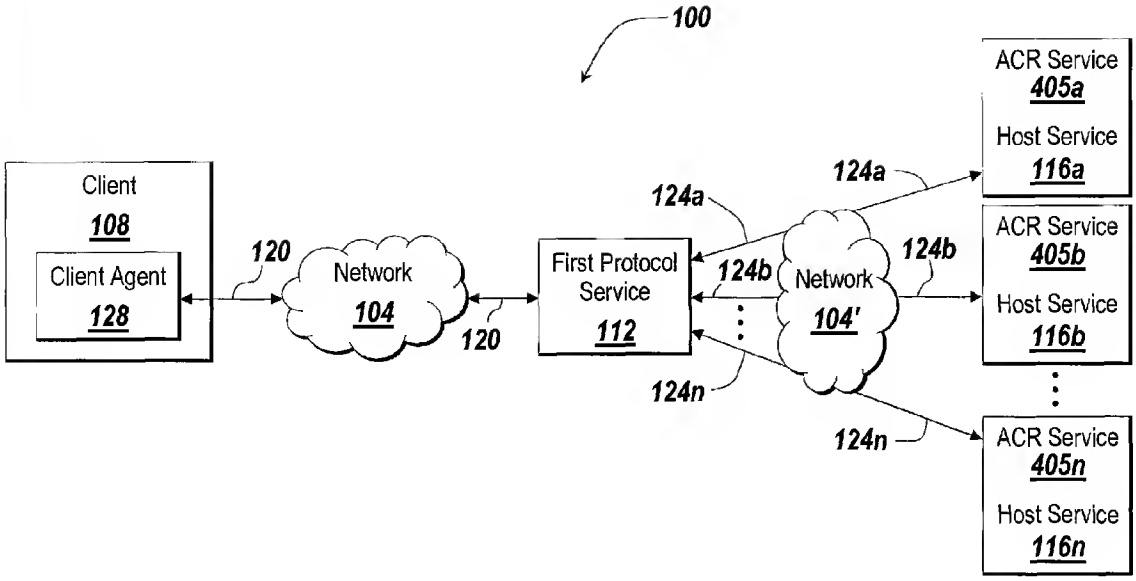
100
Client
108
Client Agent
128
120
Network
104
120
First Protocol Service
112
124a
124b
124n
Network
104'
124a
124b
124n
ACR Service
405a
Host Service
116a
ACR Service
405b
Host Service
116b
ACR Service
405n
Host Service
116n

Fig. 8A

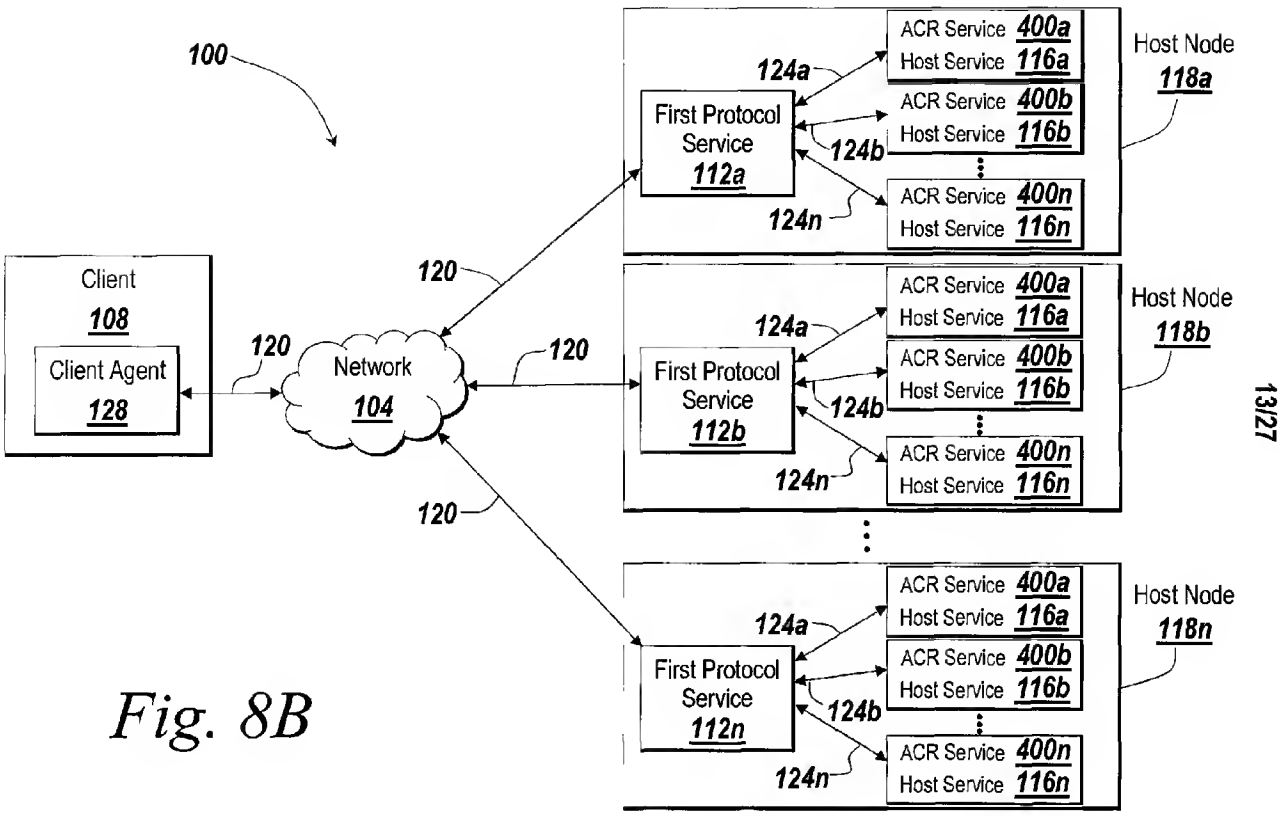
100
Client
108
Client Agent
128
120
Network
104
120
120
120
First Protocol Service
112a
First Protocol Service
112b
First Protocol Service
112n
124a
124b
124n
ACR Service 400a
Host Service 116a
ACR Service 400b
Host Service 116b
ACR Service 400n
Host Service 116n
Host Node
118a
Host Node
118b
Host Node
118n

Fig. 8B

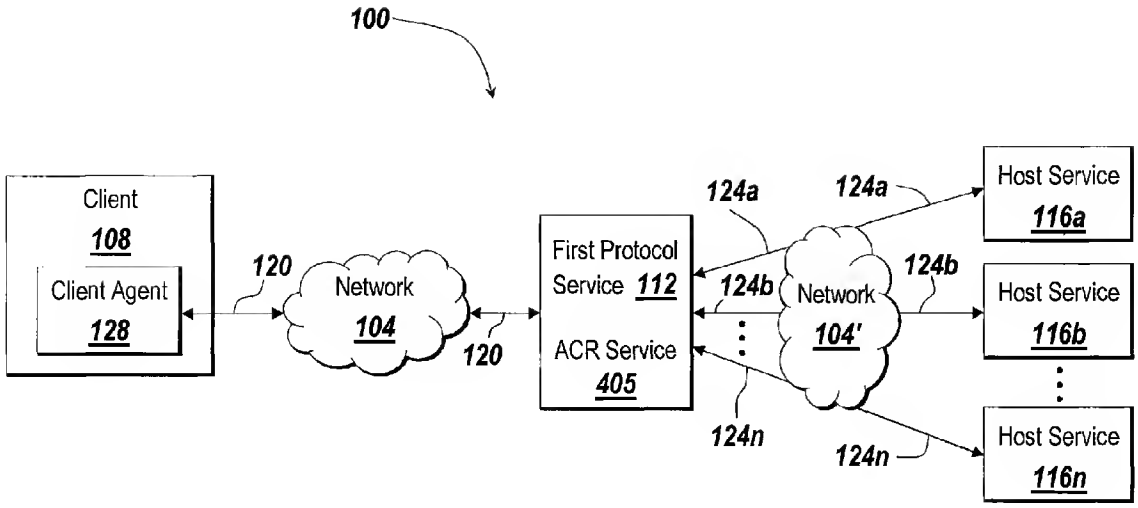
100
Client
108
Client Agent
128
120
Network
104
120
First Protocol
Service 112
ACR Service
405
124a
124b
124n
Network
104'
124a
124b
124n
Host Service
116a
Host Service
116b
Host Service
116n

Fig. 9A

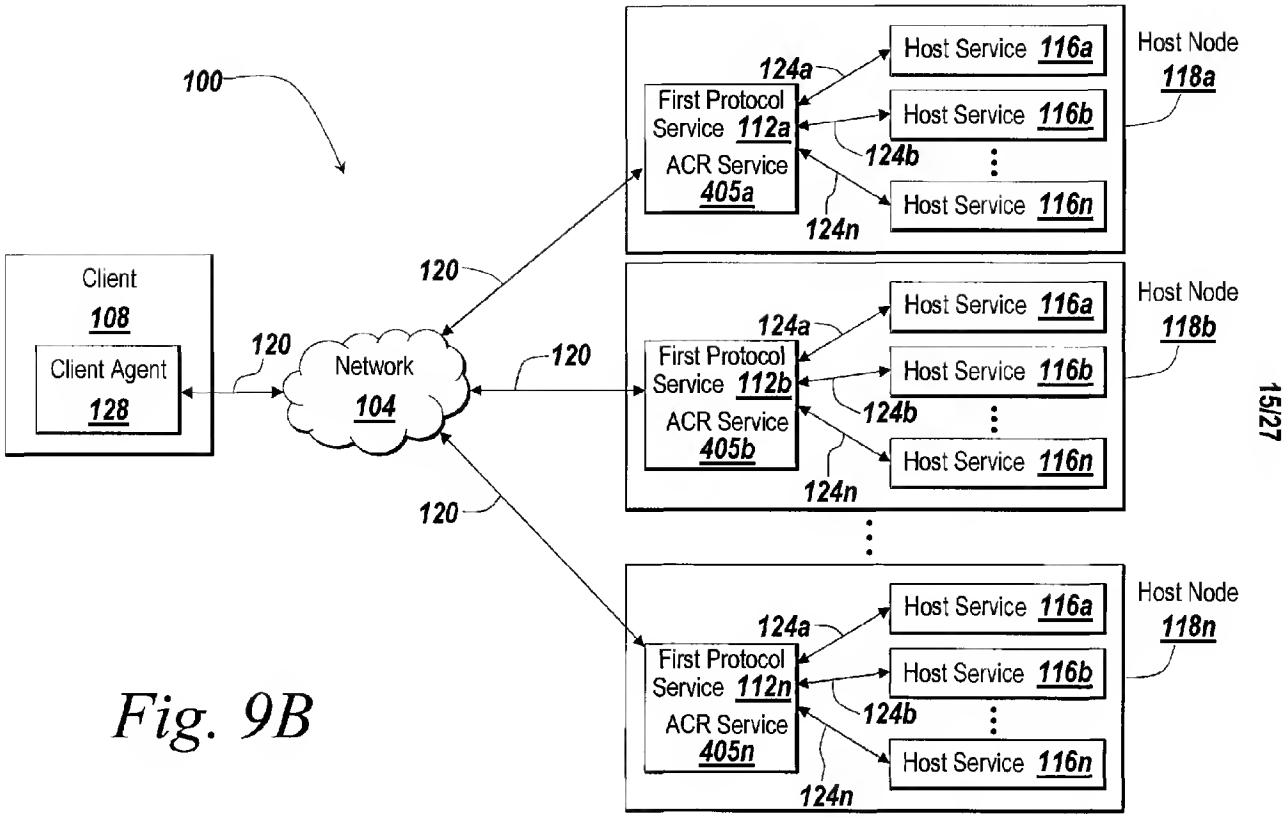
100
Client
108
Client Agent
128
120
Network
104
120
120
120
Host Node
118a
124a
First Protocol
Service 112a
ACR Service
405a
Host Service 116a
Host Service 116b
124b
Host Service 116n
124n
Host Node
118b
124a
First Protocol
Service 112b
ACR Service
405b
Host Service 116a
Host Service 116b
124b
Host Service 116n
124n
Host Node
118n
124a
First Protocol
Service 112n
ACR Service
405n
Host Service 116a
Host Service 116b
124b
Host Service 116n
124n

Fig. 9B

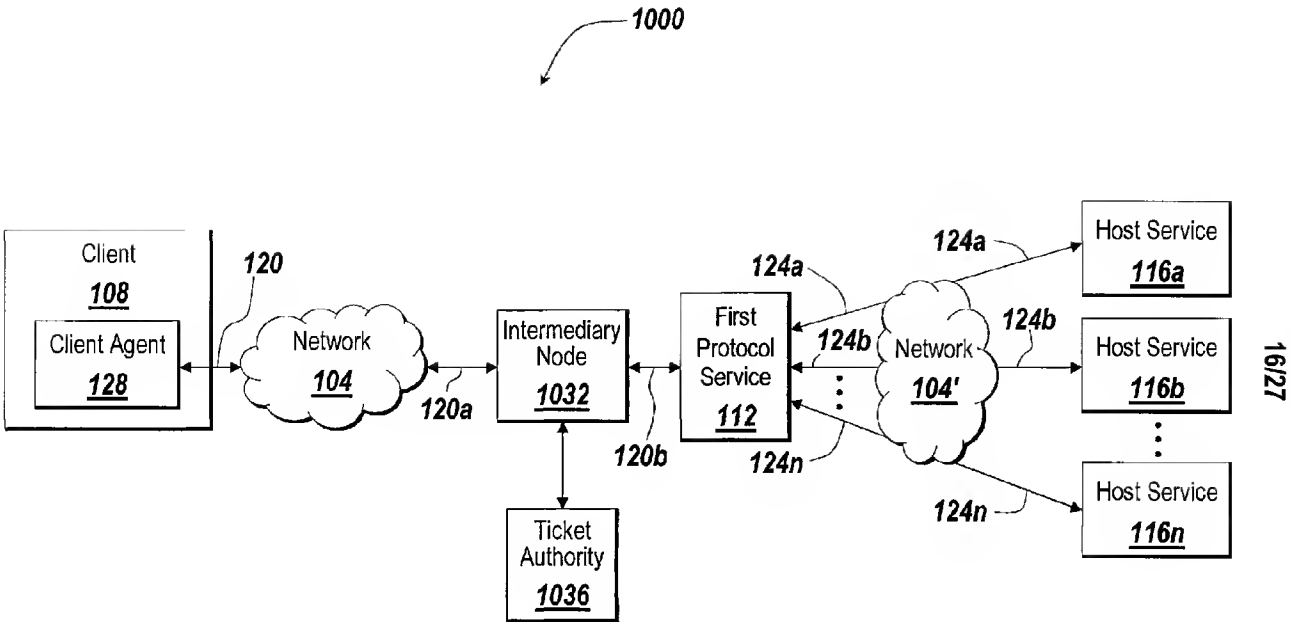
1000
Client
108
Client Agent
128
120
Network
104
120a
Intermediary Node
1032
120b
Ticket Authority
1036
First Protocol Service
112
124a
124b
124n
Network
104'
124a
124b
124n
Host Service
116a
Host Service
116b
Host Service
116n

Fig. 10A

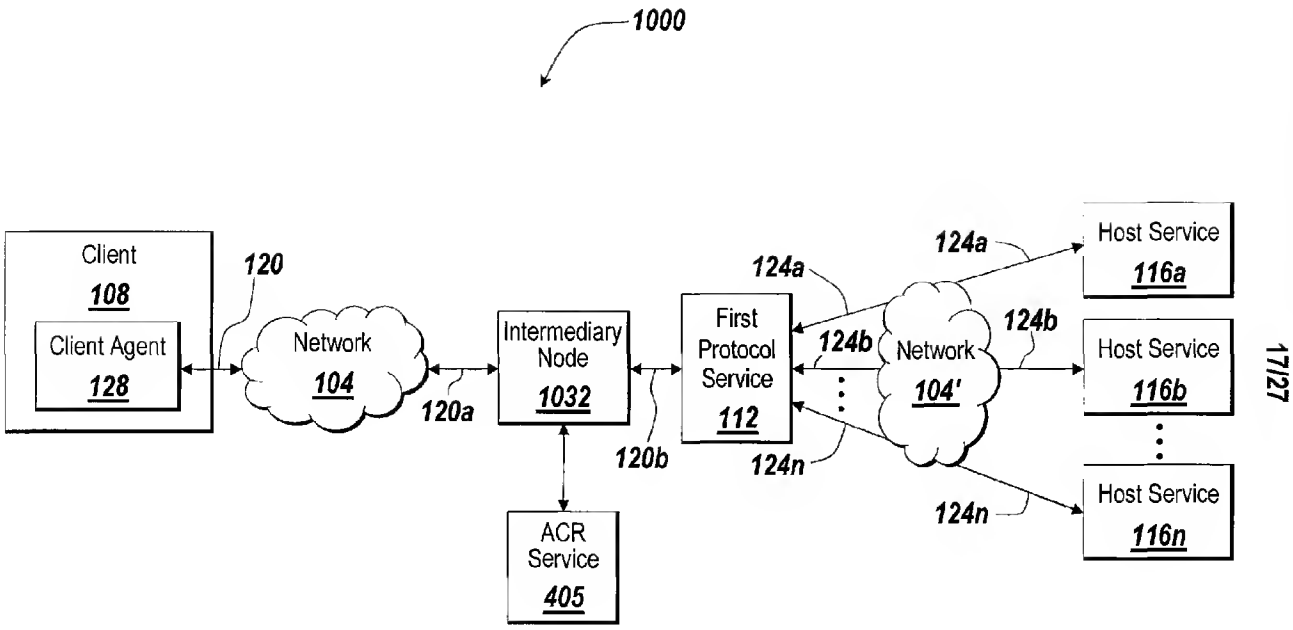
1000
Client
108
Client Agent
128
120
Network
104
120a
Intermediary Node
1032
120b
ACR Service
405
First Protocol Service
112
124a
124b
124n
Network
104'
124a
124b
124n
Host Service
116a
Host Service
116b
Host Service
116n

Fig. 10B

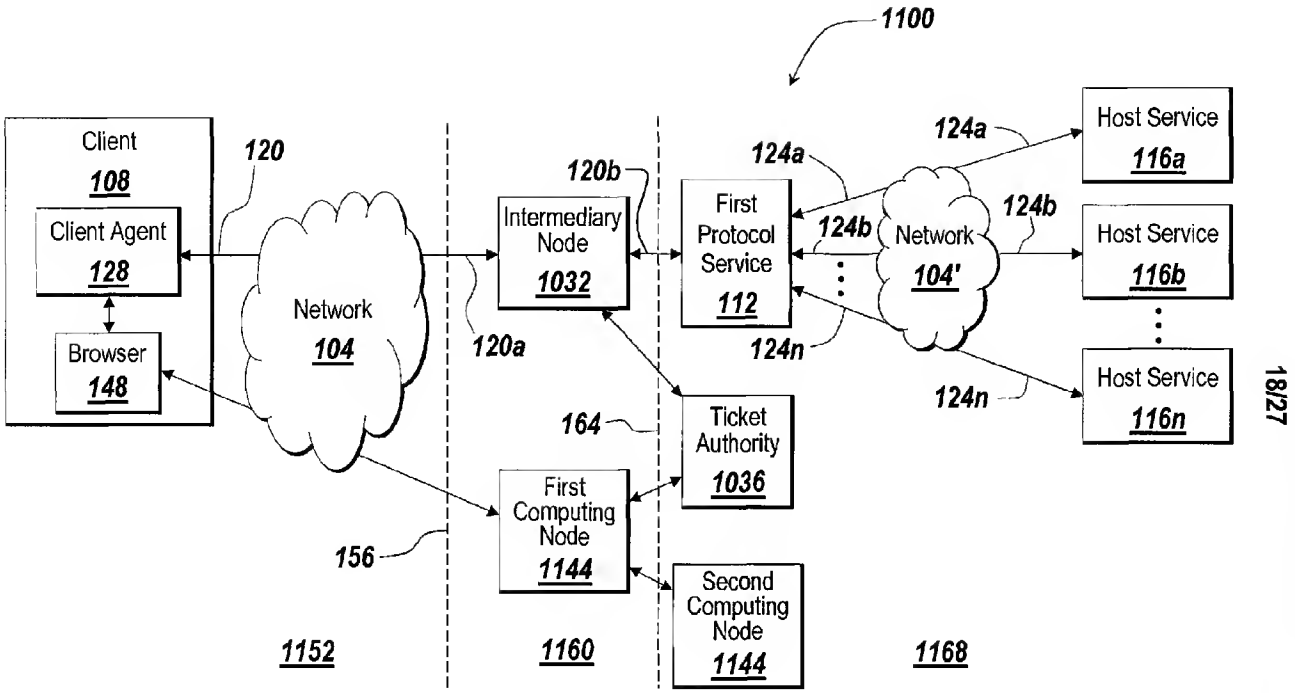
1100
Client
108
Client Agent
128
Browser
148
120
Network
104
120a
120b
Intermediary Node
1032
First Protocol Service
112
124a
124b
124n
Network
104'
Host Service
116a
Host Service
116b
Host Service
116n
164
Ticket Authority
1036
First Computing Node
1144
156
Second Computing Node
1144
1152
1160
1168

Fig. 11A

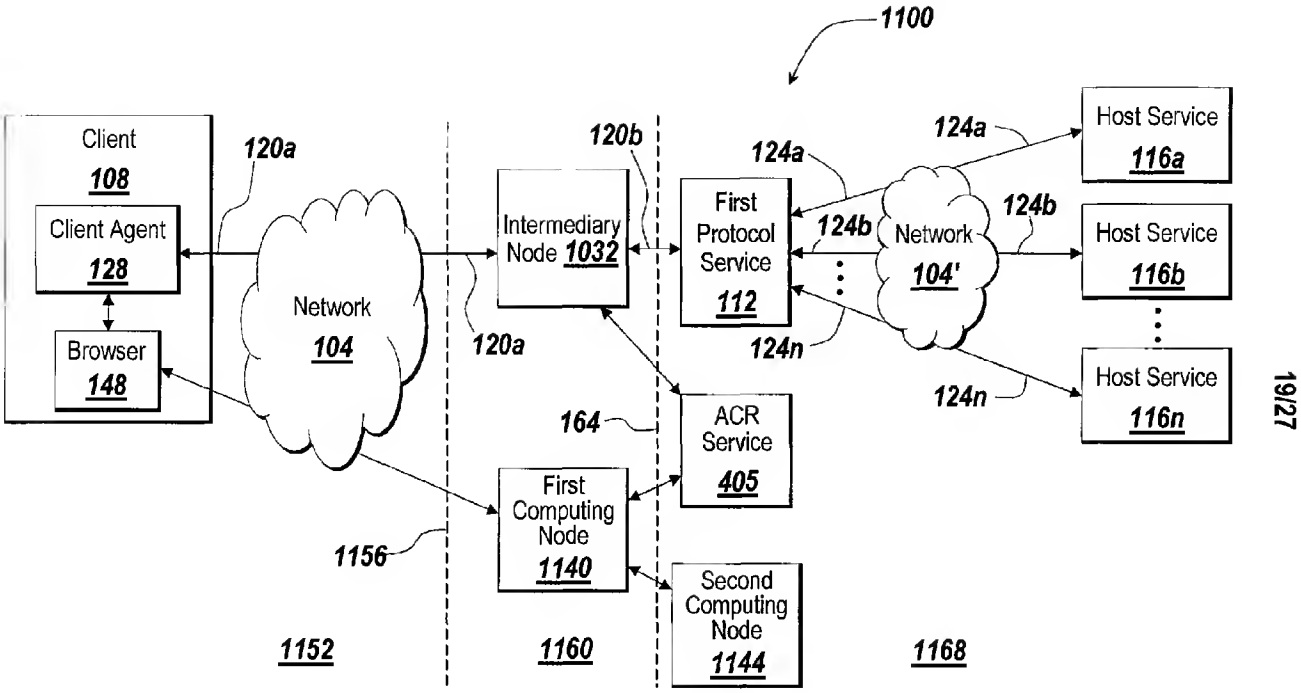
1100
Client
108
Client Agent
128
Browser
148
120a
Network
104
120a
Intermediary Node 1032
120b
First Protocol Service
112
124a
124b
124n
Network
104'
124a
124b
124n
Host Service
116a
Host Service
116b
Host Service
116n
164
ACR Service
405
First Computing Node
1140
1156
Second Computing Node
1144
1152
1160
1168

Fig. 11B

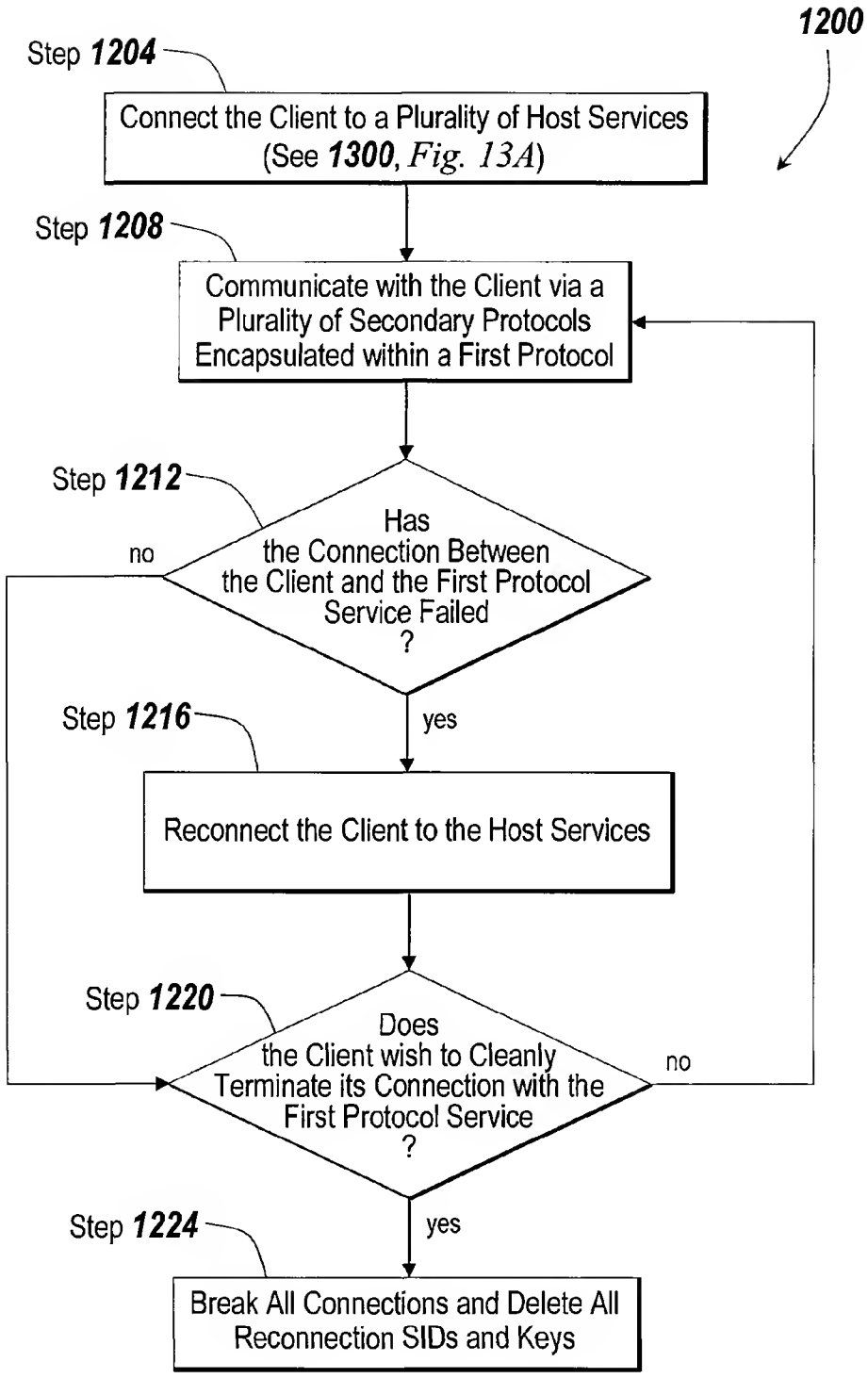
1200
Step 1204
Connect the Client to a Plurality of Host Services
(See 1300, Fig. 13A)
Step 1208
Communicate with the Client via a Plurality of Secondary Protocols Encapsulated within a First Protocol
Step 1212
Has the Connection Between the Client and the First Protocol Service Failed ?
no
yes
Step 1216
Reconnect the Client to the Host Services
Step 1220
Does the Client wish to Cleanly Terminate its Connection with the First Protocol Service ?
no
yes
Step 1224
Break All Connections and Delete All Reconnection SIDs and Keys

Fig. 12A

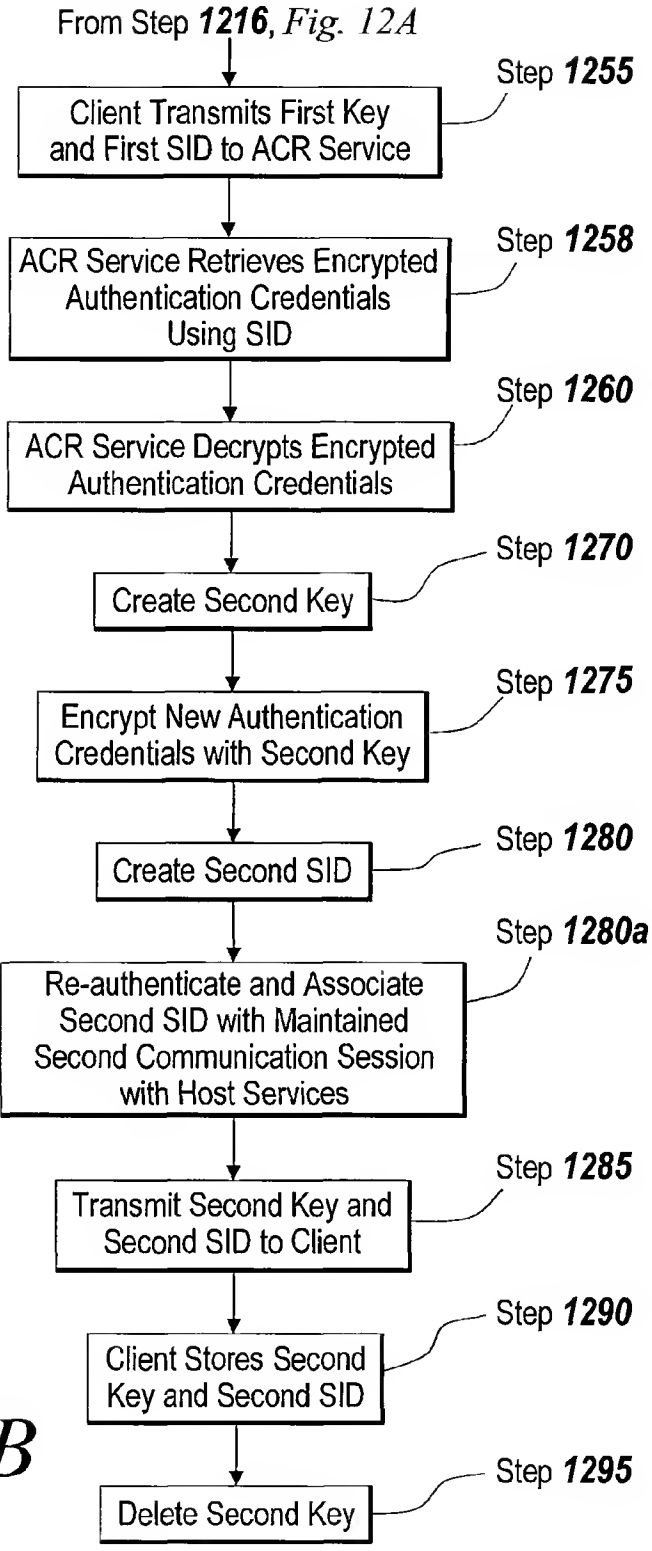
From Step 1216, Fig. 12A
Step 1255
Client Transmits First Key and First SID to ACR Service
Step 1258
ACR Service Retrieves Encrypted Authentication Credentials Using SID
Step 1260
ACR Service Decrypts Encrypted Authentication Credentials
Step 1270
Create Second Key
Step 1275
Encrypt New Authentication Credentials with Second Key
Step 1280
Create Second SID
Step 1280a
Re-authenticate and Associate Second SID with Maintained Second Communication Session with Host Services
Step 1285
Transmit Second Key and Second SID to Client
Step 1290
Client Stores Second Key and Second SID
Step 1295
Delete Second Key

Fig. 12B

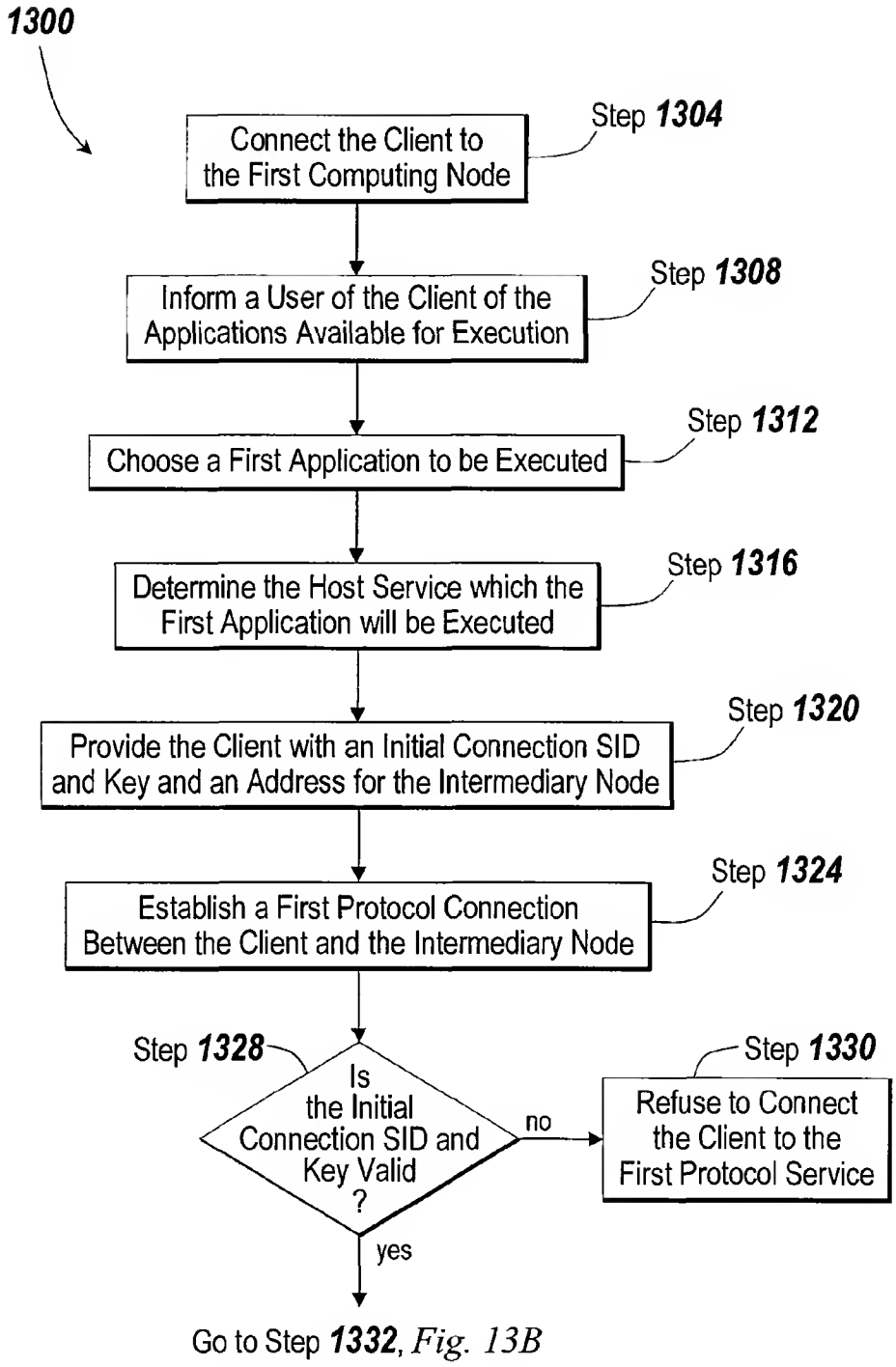
1300
Connect the Client to the First Computing Node
Step 1304
Inform a User of the Client of the Applications Available for Execution
Step 1308
Choose a First Application to be Executed
Step 1312
Determine the Host Service which the First Application will be Executed
Step 1316
Provide the Client with an Initial Connection SID and Key and an Address for the Intermediary Node
Step 1320
Establish a First Protocol Connection Between the Client and the Intermediary Node
Step 1324
Step 1328
Is the Initial Connection SID and Key Valid ?
no
Step 1330
Refuse to Connect the Client to the First Protocol Service
yes
Go to Step 1332, Fig. 13B

Fig. 13A

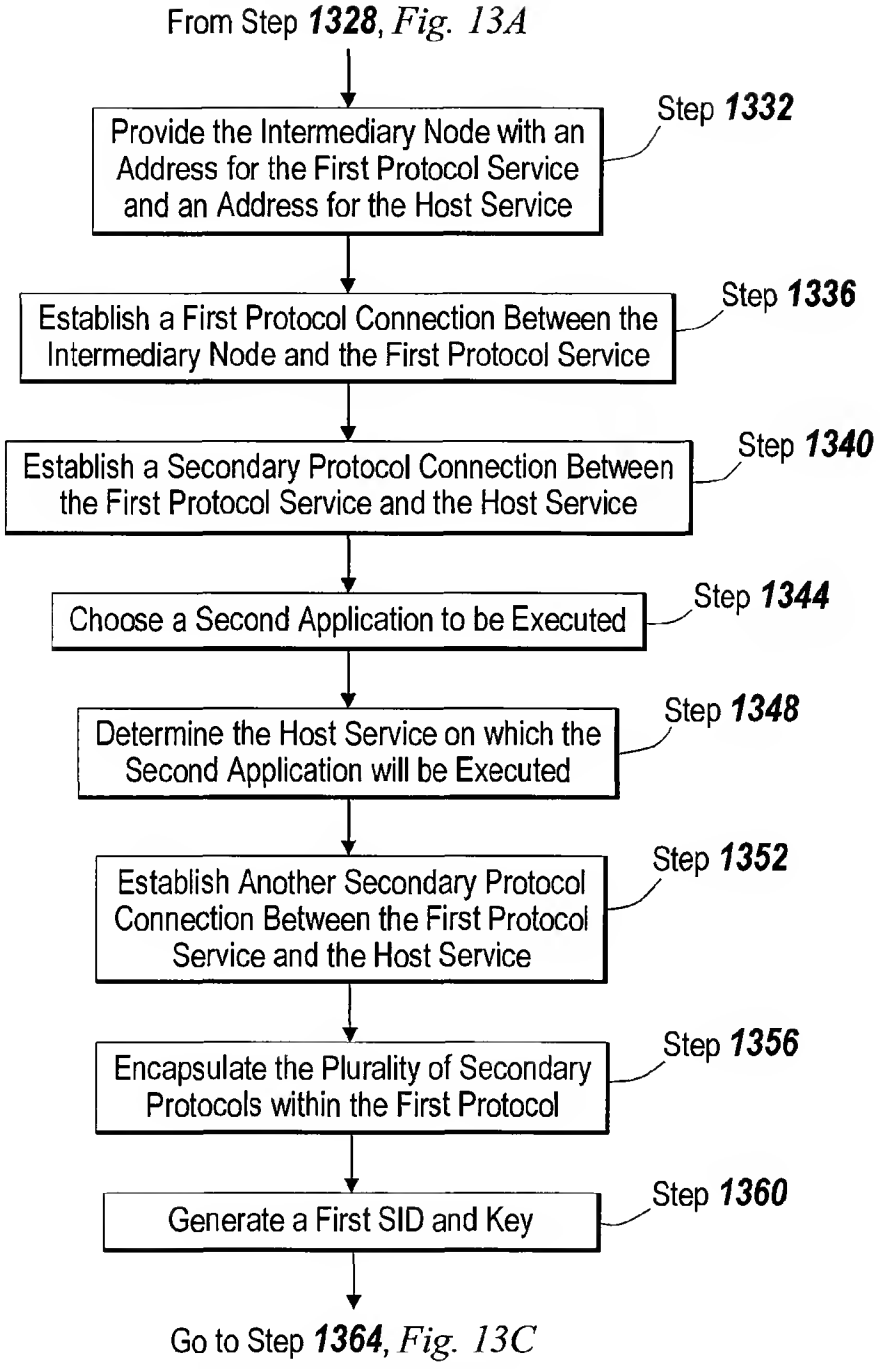
From Step 1328, Fig. 13A
Provide the Intermediary Node with an Address for the First Protocol Service and an Address for the Host Service
Step 1332
Establish a First Protocol Connection Between the Intermediary Node and the First Protocol Service
Step 1336
Establish a Secondary Protocol Connection Between the First Protocol Service and the Host Service
Step 1340
Choose a Second Application to be Executed
Step 1344
Determine the Host Service on which the Second Application will be Executed
Step 1348
Establish Another Secondary Protocol Connection Between the First Protocol Service and the Host Service
Step 1352
Encapsulate the Plurality of Secondary Protocols within the First Protocol
Step 1356
Generate a First SID and Key
Step 1360
Go to Step 1364, Fig. 13C

Fig. 13B

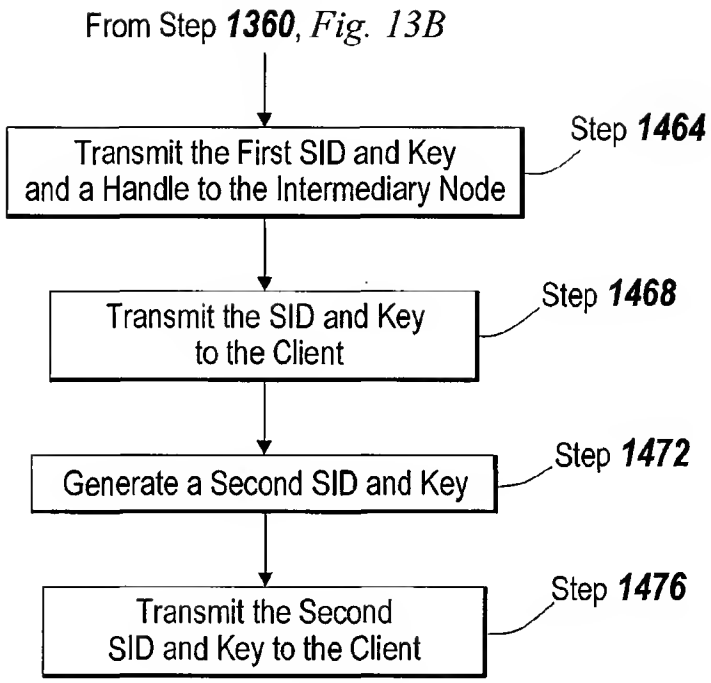
From Step 1360, Fig. 13B
Transmit the First SID and Key and a Handle to the Intermediary Node
Step 1464
Transmit the SID and Key to the Client
Step 1468
Generate a Second SID and Key
Step 1472
Transmit the Second SID and Key to the Client
Step 1476

Fig. 13C

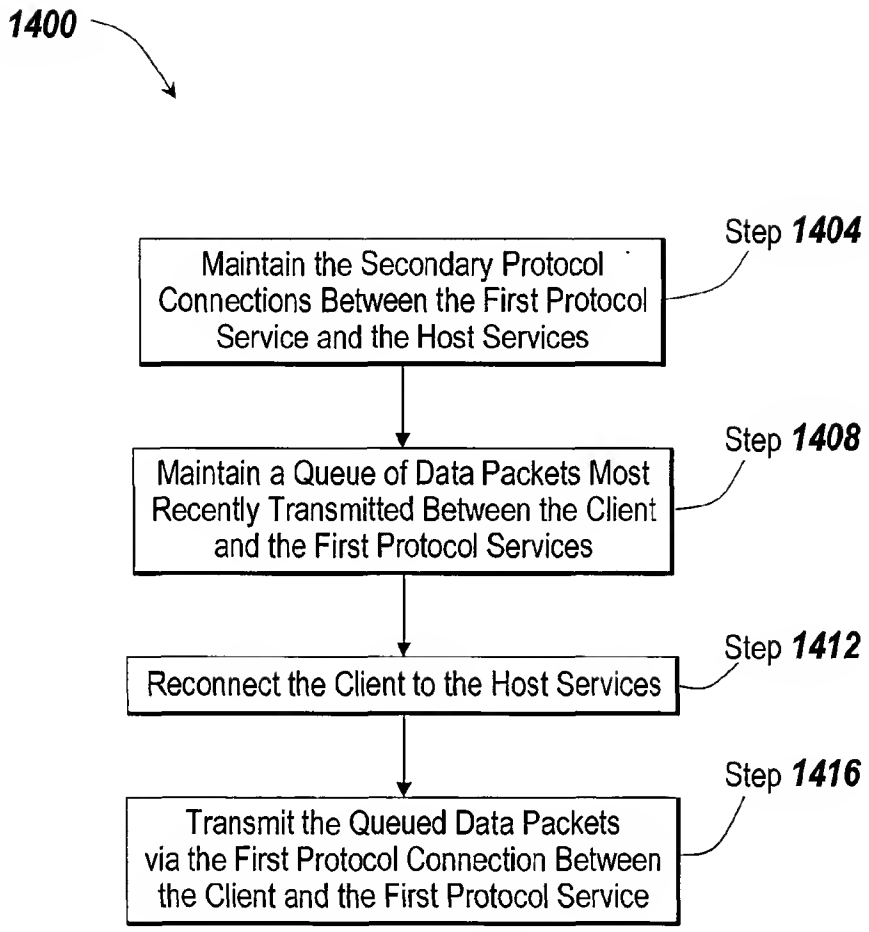
1400
Step 1404
Maintain the Secondary Protocol Connections Between the First Protocol Service and the Host Services
Step 1408
Maintain a Queue of Data Packets Most Recently Transmitted Between the Client and the First Protocol Services
Step 1412
Reconnect the Client to the Host Services
Step 1416
Transmit the Queued Data Packets via the First Protocol Connection Between the Client and the First Protocol Service

Fig. 14

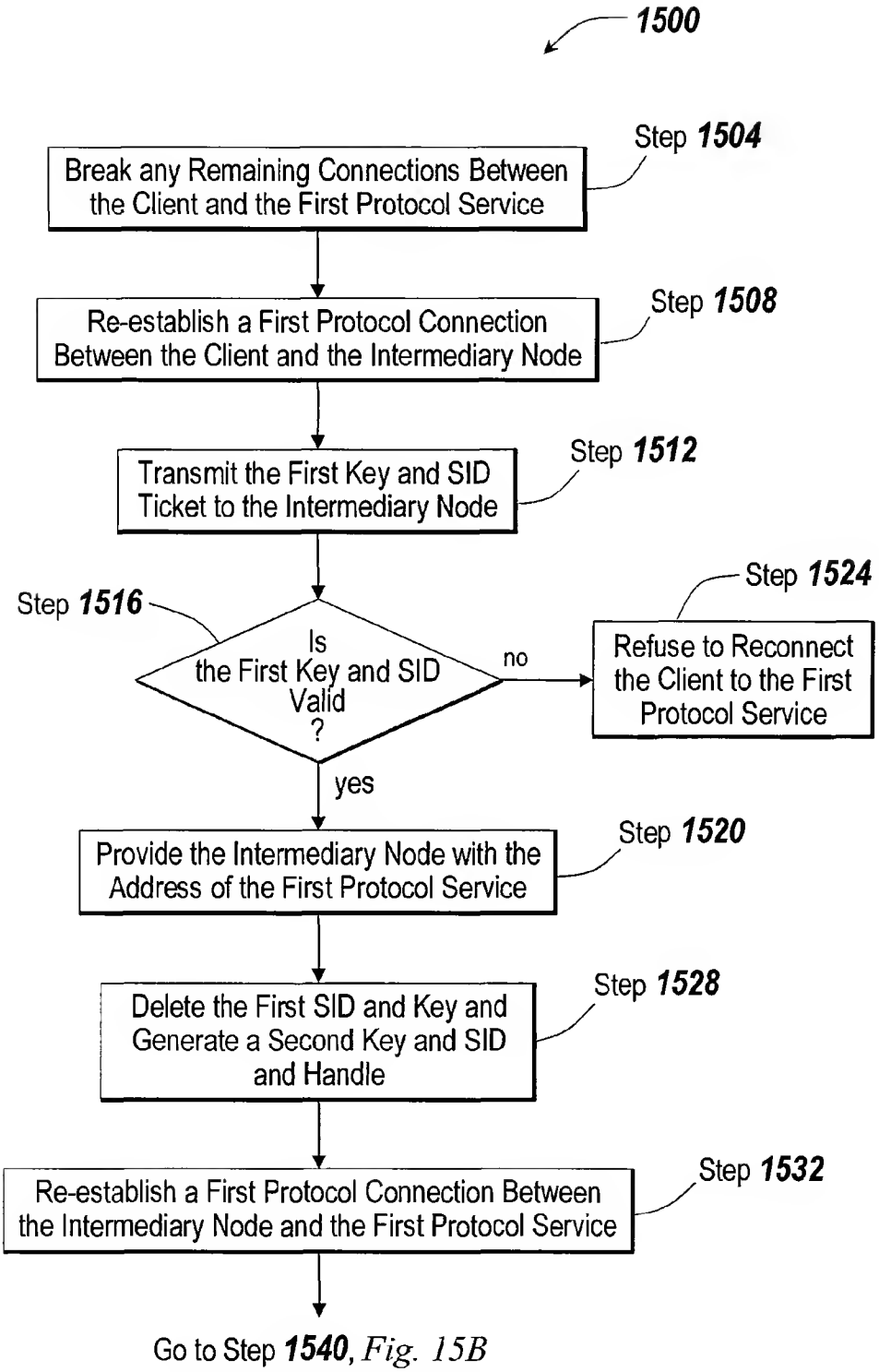
1500
Step 1504
Break any Remaining Connections Between the Client and the First Protocol Service
Step 1508
Re-establish a First Protocol Connection Between the Client and the Intermediary Node
Step 1512
Transmit the First Key and SID Ticket to the Intermediary Node
Step 1516
Is the First Key and SID Valid ?
no
Step 1524
Refuse to Reconnect the Client to the First Protocol Service
yes
Step 1520
Provide the Intermediary Node with the Address of the First Protocol Service
Step 1528
Delete the First SID and Key and Generate a Second Key and SID and Handle
Step 1532
Re-establish a First Protocol Connection Between the Intermediary Node and the First Protocol Service
Go to Step 1540, Fig. 15B

Fig. 15A

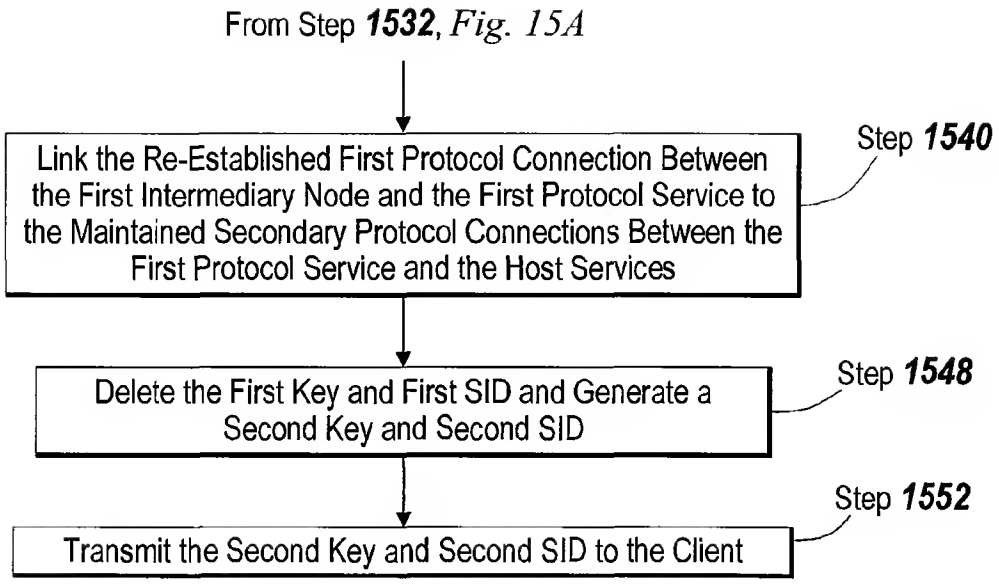
From Step 1532, Fig. 15A
Link the Re-Established First Protocol Connection Between the First Intermediary Node and the First Protocol Service to the Maintained Secondary Protocol Connections Between the First Protocol Service and the Host Services
Step 1540
Delete the First Key and First SID and Generate a Second Key and Second SID
Step 1548
Transmit the Second Key and Second SID to the Client
Step 1552

Fig. 15B